PTO/SB/17 (07-06)
Approved for use through 01/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	10/082,186-Conf. #4346
Filing Date	February 26, 2002
First Named Inventor	Akira Kimura
Examiner Name	M. J. Pyzocha
Art Unit	2137
Attorney Docket No.	SON-2356

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order □ None □ Other (please identify): ____________

☒ Deposit Account Deposit Account Number: 18-0013 Deposit Account Name: Rader, Fishman & Grauer PLLC

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below □ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fee ($)**	**Small Entity Fee ($)**	**Fees Paid ($)**
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	**Fee ($)**	**Small Entity Fee ($)**
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims ______ - ______ = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ______ - ______ = **Extra Claims** ______ x **Fee ($)** ______ = **Fee Paid ($)** ______

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims

Fee ($) ______ **Fee Paid ($)** ______

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ______ - 100 = **Extra Sheets** ______ /50 **Number of each additional 50 or fraction thereof** ______ (round up to a whole number) x **Fee ($)** ______ = **Fee Paid ($)** ______

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): 1402 Filing a brief in support of an appeal	500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	40,290	Telephone	(202) 955-3750
Name (Print/Type)	Christopher M. Tobin			Date	January 17, 2007

TRANSMITTAL OF APPEAL BRIEF	Docket No. SON-2356

In re Application of: Akira Kimura

Application No.	Filing Date	Examiner	Group Art Unit
10/082,186-Conf. #4346	February 26, 2002	M. J. Pyzocha	2137

Invention: AUTHENTICATION SYSTEM AND METHOD, IDENTIFICATION INFORMATION INPUTTING METHOD AND APPARATUS ANDS PORTABLE TERMINAL

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: November 17, 2006 .

The fee for filing this Appeal Brief is $ 500.00 .

☒ Large Entity □ Small Entity

□ A petition for extension of time is also enclosed.

The fee for the extension of time is ______ .

□ A check in the amount of ______ is enclosed.

☒ Charge the amount of the fee to Deposit Account No. 18-0013 .
This sheet is submitted in duplicate.

□ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 18-0013 .
This sheet is submitted in duplicate.

Dated: January 17, 2007

Christopher M. Tobin
Attorney Reg. No. : 40,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750

Docket No.: SON-2356
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Akira Kimura

Application No.: 10/082,186

Confirmation No.: 4346

Filed: February 26, 2002

Art Unit: 2137

For: AUTHENTICATION SYSTEM AND METHOD, IDENTIFICATION INFORMATION INPUTTING METHOD AND APPARATUS AND PORTABLE TERMINAL

Examiner: M.J. Pyzocha

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is an Appeal Brief under 37 C.F.R. § 41.37 appealing the final decision of the Examiner dated August 23, 2006. This Brief is in furtherance of and is filed within two months of the Notice of Appeal filed on November 17, 2006.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Sony Corporation, of Tokyo, Japan. An assignment of all rights in the present application to Sony was executed by the inventors and recorded by the United States Patent and Trademark Office at Reel 013090, Frame 0367.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Current Status of Claims

A complete listing of the claims with corresponding status is provided as follows:

Claim 1. (Rejected).

Claim 2. (Rejected).

Claim 3. (Rejected).

Claim 4. (Rejected).

Claim 5. (Rejected).

Claim 6. (Rejected).

Claim 7. (Rejected).

Claim 8. (Rejected).

Claim 9. (Rejected).

Claim 10. (Rejected).

Claim 11. (Rejected).

Claim 12. (Rejected).

Claim 13. (Rejected).

Claim 14. (Rejected).

Claim 15. (Rejected).

Claim 16. (Rejected).

Claim 17. (Rejected).

Claim 18. (Rejected).

Claim 19. (Rejected).

Claim 20. (Rejected).

Claim 21. (Rejected).

Claim 22. (Rejected).

Claim 23. (Rejected).

Claim 24. (Rejected).

Claim 25. (Canceled).

Claim 26. (Canceled).

Claim 27. (Canceled).

Claim 28. (Canceled).

Claim 29. (Canceled).

Claim 30. (Canceled).

Claim 31. (Canceled).

Claim 32 (Canceled).

Claim 33 (Canceled).

Claim 34 (Canceled).

Claim 35 (Rejected).

Claim 36 (Rejected).

Claim 37 (Rejected).

Claim 38 (Rejected).

Claim 39 (Rejected).

Claim 40 (Rejected).

Claim 41 (Rejected).

Claim 42 (Rejected).

Claim 43 (Rejected).

Claim 44 (Rejected).

Claim 45 (Rejected).

Claim 46 (Rejected).

B. Claims On Appeal

Appellant hereby appeals the final rejection of claims 1-24 and 35-46.

IV. STATUS OF AMENDMENTS

Following the Final Rejection dated August 23, 2006, a Response to the Final Office Action was filed on October 16, 2006. The Response was a request for reconsideration traversing the rejections of record, with no amendments to the claims. An Advisory Action was mailed on October 26, 2006, wherein the Examiner indicated that the request for reconsideration had been considered, but was deemed not to place the application in condition for allowance, with an appended explanation.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following description is for illustrative purposes and is not intended to limit the scope of the invention.

The present invention relates to preventing unauthorized acquisition of private information by a third party in the course of authentication of a user by a service provider. (Abstract). The claims variously recite apparatus, methods and computer program products for avoiding such contentious assignment of addresses.

Independent claim 1 recites: [a]n authentication system, said authentication system comprising:

a portable card terminal (*e.g.*, FIGs. 2-3, element 10), including:

first identification information storage means (*e.g.*, FIGs. 2-3, element 11) having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information (*e.g.*, FIGs. 2-3, element 12),

encryption means for encrypting the second identification information input by said operating means based on encryption key information (*e.g.*, FIGs. 2-3, element 14), and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication_device in response to transmitting the first identification information (*e.g.*, FIGs. 2-3, element 13);

said authentication device (*e.g.*, FIGs. 2-3, element 20), provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein (*e.g.*, FIGs. 2-3, element 23),

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal (*e.g.*, FIGs. 2-3, element 22),

second communication means for communication with said portable card terminal (*e.g.*, FIGs. 2-3, element 21), and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information (*e.g.*, FIGs. 2-3, element 25);

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device (*e.g.*, FIGs. 2-3, element 10, FIG. 1, S4, specification p. 22); and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication (*e.g.*, FIGs. 2-3, element 20; FIG. 1, S5; specification p. 23).

Independent claim 13 recites: [a]n authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable card terminal, said method comprising

an operating step of inputting a second identification information associated with a first identification information that discriminates said portable card terminal and that is stored in a first identification information storage means of said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal (*e.g.*, FIG. 1, S1 and related description)

an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device (*e.g.*, FIG. 1, S2 and related description), and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal (e.g, FIG. 1, S3 and related description),

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step (*e.g.*, FIG. 1, S4 and related description), and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to the second identification information as stored in a second identification information storage means to perform the authentication (*e.g.*, FIG. 1, S5 and related dscription).

Independent claim 35 recites: [a] portable card terminal (*e.g.*, FIGs. 2-3, element 10) authenticated by an authentication device (*e.g.*, FIGs. 2-3, element 20) , comprising, first identification information storage means for storing a first identification information for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal (*e.g.*, FIGs. 2-3, element 11),

operating means for inputting a second identification information associated with said first identification information (*e.g.*, FIGs. 2-3, element 12),

communication means for communication with said authentication device wherein said communication including transmitting the first identification information from the portable card terminal to the authentication device, and receiving encryption key information from the authentication device in response to transmitting the first identification information (*e.g.*, FIGs. 2-3, element 13), and

encrypting means for encrypting the second identification information input by said operating means based on said encryption key information received from said authentication device, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal (*e.g.*, FIGs. 2-3, element 14).

Independent claim 46 recites: [a]n authentication system (*e.g.*, FIGs. 2-3, element 1) made up by a portable card terminal (*e.g.*, FIGs. 2-3, element 10) and an authentication device (*e.g.*, FIGs. 2-3, element 20) provided independently of said portable card terminal for communication with said portable card terminal, said authentication system comprising:

said portable card terminal (*e.g.*, FIGs. 2-3, element 10), including

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal (*e.g.*, FIGs. 2-3, element 11), operating means including display means for irregularly displaying letters included in a group of letters and selection means for selecting the letters making up a second identification information from among the letters irregularly displayed on said display means, said operating means inputting the second identification information associated with said first identification information (*e.g.*, FIGs. 2-3, element 12; FIG. 4),

encryption means for encrypting the second identification information input by said operating means based on an encryption key information (*e.g.*, FIGs. 2-3, element 14), and

first communication means for communication with said authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information (*e.g.*, FIGs. 2-3, element 13);

said authentication device (*e.g.*, FIGs. 2-3, element 20), including

second identification information storage means having the first identification information and the second identification information stored therein (*e.g.*, FIGs. 2-3, element 23),

encryption key information generating means for generating said encryption key information, wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal (*e.g.*, FIGs. 2-3, element 22),

second communication means for communication with said portable card terminal (*e.g.*, FIGs. 2-3, element 21), and

comparator authentication means for comparing the second identification information encrypted by said encryption means to the second identification information stored in the second identification information storage means (*e.g.*, FIGs. 2-3, element 25); wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device through said first communication means, and the so-encrypted second identification information is transmitted through said first communication means to said authentication device (*e.g.*, FIGs. 2-3, element 10, FIG. 1, S4, specification p. 22); and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication (*e.g.*, FIGs. 2-3, element 10, FIG. 1, S5, specification p. 23).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for consideration in this appeal are as follows:

Whether the Examiner erred in rejecting claims 1-9, 13-21 and 35-42 under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky") in view of B. Schneier, "Applied Cryptography," John Wiley & Sons, 1996, pp. 33-34 ("Schneier II")

Whether the Examiner erred in rejecting claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of U.S. Pat. No. 6,195,698 to Lillibridge ("Lillibridge").

These issues are discussed in the following section.

VII. ARGUMENT

In the Final Office Action of August 23, 2006, the Examiner erred in rejecting claims 1-9, 13-21 and 35-42 under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,880,769 to Nemirofsky et al. ("Nemirofsky") in view of B. Schneier, "Applied Cryptography," John Wiley & Sons, 1996, pp. 33-34 ("Schneier II"), and erred in rejecting claims claims 10-12, 22-24, and 43-46 under 35 U.S.C. 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of U.S. Pat. No. 6,195,698 to Lillibridge et al. ("Lillibridge").

Grouping of claims: Claims 1-24 and 35-46 are currently pending in the application. Claims 1-5 and 35-38 stand or fall together. Claims 13-17 stand or fall together. Claims 6, 18 and 39 stand or fall together. Claims 7, 19 and 40 stand or fall together. Claims 8, 20 and 41 stand or fall together. Claims 9, 21 and 42 stand or fall together. Claims 10-12, 22-4 and 43-46 stand or fall together.

The Examiner erred in rejecting claims 1-9, 13-21 and 35-42 under 35 U.S.C. 103(a) as being unpatentable over Nemirofsky in view of Schneier II:

Independent claim 1 recites: *[a]n authentication system, said authentication system comprising:*

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein, *encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,*

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

Appellant's claimed invention provides a technique for protecting unauthorized access to private information in a situation where the user accesses information using a portable card terminal that communicates with an authentication system. Independent claim 1 recites authentication features involving the first identification information (*e.g.*, the portable card terminal ID), correlated generation of an encryption key, and encryption of second identification information input to the portable card terminal using the encryption key. Specifically, the claim recites authentication wherein (1) the "first identification information" (further recited as the portable card ID) is sent from the portable card terminal to the authentication device, (2) the authentication device generates the encryption key in response to receiving the first identification information, (3) the authentication device sends the so-generated encryption key back to the portable terminal device, and (4) the portable terminal device then uses the encryption key to encrypt second identification information input to the portable card terminal (*e.g.*, the PIN entered by the user) and sends this encrypted second identification information to the authentication device, which then performs authentication.

Neither Nemirofsky nor Schneier II disclose the claimed features of Appellant's invention, whether taken alone or in any combination.

Nemirofsky fails to disclose numerous features of Appellant's claimed invention:

Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security. Nemirofsky makes no mention of encrypting the PIN code. In that sense, Nemirofsky appears to disclose a typical banking card type exchange, wherein the user enters the PIN code and that information allows the user to continue access to financial or other information. There is no mention of encrypting the PIN code even generally, let alone according to the specific exchange of information claimed by Appellant.

The Examiner admits that Nemirofsky does not disclose encrypting based upon an encryption key received from an authentication device. (Final Office Action dated 8/23/06, at p. 3). Appellant concurs with this conclusion. However, Appellant submits that this is a simplification of the deficiencies of Nemirofsky, as various claimed features are absent from that reference.

Nemirofsky discloses a smart card, and discloses that a PIN may be used in association with usage of the smart card, but makes no mention with regard to ***any*** encryption technique for that PIN, let alone the particular sequence claimed by Appellant. In fact, the entirety of the above-described sequence of Appellant's claimed invention is absent from Nemirofsky. At best, Nemirofsky uses a PIN that is sent to the authentication device. There is no mention in the reference of (1) sending the "first identification information" (the portable card ID) from the portable card terminal to the authentication device, (2) having the authentication device generate the encryption key in response to receiving the first identification information, (3) having the authentication send the so-generated encryption key back to the portable terminal device, (4) then having the portable terminal device use the encryption key to encrypt second identification information that is input to the portable card terminal (*e.g.*, the PIN entered by the user) and send the encrypted second identification information to the authentication device, which finally performs authentication.

The Examiner characterizes Nemirofsky as merely omitting feature (2), but the various other features of Appellant's claimed invention are also clearly absent from the reference. At most, Nemirofsky discloses a smart card and corresponding PIN code for using the smart card. There is no mention of encrypting the PIN, nor is there any mention of first sending the portable card ID to the authentication device, then having the authentication device generate a corresponding encryption code, then sending that back to the smart card for usage in encrypting the PIN code.

In the Advisory Action dated 10/26/06, the Examiner states that Nemirofsky teaches the use of encryption in the smartcard system, with reference to column 1 line 63 through column 2 line 3, and column 4, lines 20-25, which are said to disclose RSA and DES algorithms. The two passages that the Examiner cites merely confirm what Appellant states above, which is that the reference fails to even disclose generally the encrypting of the PIN code, let alone the remaining elements of the authentication sequence. Specifically, these passages state that data that is sent to the IC card may be encrypted for security, and that non-visual data encoded using the VEIL protocol data may also be encrypted. Neither of these passages in any way discloses or suggests encrypting the PIN code, or of engaging in the particular sequence for generating an encryption key to do so, based upon the portable card identifier, as described above.

Schneier does not remedy the deficiencies of Nemirofsky:

The Examiner generally refers to "pages 33-34" of Schneier, but Appellant does not believe that anything contained therein discloses the claimed features noted above. In Schneier II, public-key cryptography, and particularly an example of a "hybrid cryptosystem" is described. This description does not disclose or suggest Appellant's claimed invention. With regard to this, Schneier II offers the following example:

"(1) Bob sends Alice his public key

(2) Alice generates a random session key, K, encrypts it using Bob's public key, and sends it to Bob. EB(K)

(3) Bob decrypts Alice's message using his private key to recover the session key. DB(EB(K))=K

(4) Both of them encrypt their communications using the same session key."

(Schneier II, at p. 33).

This is clearly distinct from, and offers no disclosure or suggestion of the particular features claimed by Appellant. The disclosed technique offers a way to send an encrypted session key from user A to user B, with user B being able to decrypt the session key using a private key. There is no disclosure of the particular authentication features claimed by Appellant. With Appellant's claimed invention the card ID is sent to the authentication device, then the authentication device generates the encryption key information and forwards the so-generated encryption key information to the portable card terminal. Only then does the portable card terminal encrypt the second identification information that has been input, using the so-generated encryption key information. There is no disclosure or suggestion of these particular features of Appellant's claimed invention, in either of the relied upon references, or in any combination thereof.

The Examiner has previously cited Nemirofsky's disclosure of a smart card serial number as a possible portable card identifier as claimed. However, even assuming this to be correct, there still would be no disclosure or suggestion of the claimed authentication features. Appellant reiterates that concluding as such would require significant conjecture, even in light of Schneier II. That is, one would have to conclude that the smart card serial number is sent out, that an encryption key is then generated and then returned to the smart card, with the smart card then using that encryption key to encrypt the PIN number.

Given that Nemirofsky does not even generally disclose encrypting the PIN number, it cannot be fairly concluded that the disclosure of public-key cryptography techniques by Schneier II would disclose, suggest, or in any way motivate the artisan to provide such features. Schneier II discloses receipt of a public key, which is used to encrypt a session key, and corresponding decryption of the session key based upon a previously held private key. These features do not disclose or suggest generating and returning an encryption key in association with a received portable card terminal identifier, and then encrypting second information that is input to the portable card terminal using the so-generated encryption key.

Schneier II thus clearly fails to remedy the deficiencies of Nemirofsky.

Schneier II teaches away from Appellant's claimed invention:

Schneier II teaches away from Appellant's claimed invention, because it states that public-key algorithms are appropriate for encrypting keys rather than messages. With regard to public-key algorithms, Schneier II states that:

> "[i]n the real world, public-key algorithms are not a substitute for symmetric algorithms. They are not used to encrypt messages, they are used to encrypt keys."

(Schneier II, at p. 33).

Thus, in addition to failing to specify the sequence that is absent from Nemirofsky, Schneier II suggests that the disclosed public-key algorithms are not even relevant to the type of information that is encrypted in accordance with Appellant's claimed invention. That is, with Appellant's claimed invention, information that is input to the portable card terminal is encrypted. This is clearly in contrast, even generally, to the encryption of a session key.

There is no proper motivation to combine the relied upon references:

It is also noted that a proper motivation to combine the references in the offered fashion is absent. *Prima facie* obviousness of a claimed invention is established "only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). There are three possible sources for a motivation to combine references: 1) the nature of the problem to be solved, 2) the teachings of the prior art, and 3) the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1358, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998).

Here, there is no express, implied or any kind of apparent motivation for the artisan to modify Nemirofsky according to the teachings of Schneier. As described above, there is no mention of encrypting the PIN code of Nemirofsky. Therefore, one would not look to specific techniques given that there is no general suggestion to even consider such a modification. Also, one first considering the teachings of Schneier would in no way be motivated to look to Nemirofsky. Schneier makes no mention of applying the disclosed techniques to situations where a portable card terminal interfaces with an authentication system, and makes no mention of the desirability of generating an encryption code based upon a card ID, or of encrypting a user-entered PIN code. There is clearly no objectively reasonable reason that one would conclude that the artisan would be motivated to combine the relied upon references in the fashion envisioned (in hindsight) by the Examiner.

<u>There is no prima facie case of obviousness, regardless of whether proper motivation to combine is assumed</u>:

Appellant submits that, even assuming for the sake of argument that motivation to combine the references is present, a *prima facie* case of obviousness remains absent. This is because even a combination of the references would still fail to yield various features of the claimed invention. Appellant submits that the Examiner's case for obviousness entirely relies upon conjecture and that the features recited in detail above are clearly absent from the references, even in combination.

For reasons similar to those provided regarding claim 1, independent claim 35 is also neither disclosed nor suggested by the relied upon references.

Independent claim 13 recites: *[a]n authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable card terminal, said method comprising*

an operating step of inputting a second identification information associated with a first identification information that discriminates said portable card terminal and that is stored in a first identification information storage means of said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device, and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal,

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step, and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to the second identification information as stored in a second identification information storage means to perform the authentication.

Nemirofsky and Schneier II fail to disclose or suggest various features recited in independent claim 13, including but not limited to "an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device, and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal," and " an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step."

Dependent claims 2-9, 14-21 and 39-42 are neither disclosed nor suggested for their incorporation of the features respectively recited in the independent claims as described above. Moreover, the dependent claims include their own separately recited features that are neither disclosed nor suggested by the relied upon references.

With regard to claims 6, 18 and 39, the relied upon references clearly fail to disclose or suggest "wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently."

With regard to claim 7, 19 and 40 the relied upon references clearly fail to disclose or suggest "wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device."

With regard to claims 8, 20 and 41, the relied upon references clearly fail to disclose or suggest "wherein said second identification information stored in said transient storage means is erased every preset time interval."

Finally, with regard to claims 9, 21 and 42, the relied upon references clearly fail to disclose or suggest "wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means."

Appellant respectfully requests reversal of the Examiner's rejection of claims 1-9, 13-21 and 35-42 under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II.

The Examiner erred in rejecting claims 10-12, 22-24, and 43-46 under 35 U.S.C. 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of Lillibridge:

Claims 10-12, 13-21 and 35-42 respectively depend from the independent claims discussed above, and thus incorporate the features recited therein. Claim 46 is drafted in independent form, but recites features similar to those presented in the independent claims described above, as well as additional features.

Lillibridge is relied upon as purportedly disclosing the irregular display of letters and corresponding receipt of input from such displayed letters. However, the Examiner does not allege, and Appellant notes, that Lillibridge does not remedy the above-described deficiencies of Nemirofsky and Schneier II in that it also fails to disclose or suggest sending the portable card ID, generating the corresponding encryption code, and encrypting the second information input by the user as recited in each of the independent claims. Accordingly, the combination of Nemirofsky, Schneier II and Lillibridge fails to produce Appellant's claimed invention as recited in the independent claims described above.

In addition to the above-described deficiencies, Lillibridge does not disclose the additional features recited in the dependent claims. Lillibridge discloses the generation of random sequences of characters, which can then be input in some fashion, such as shown in FIG. 4 of Lillibridge. Lillibridge is devoid of any disclosure of plural input units having ***arraying positions*** that are variable. Thus, Lillibridge does not disclose or suggest the additional features of "wherein said operating means in said portable card terminal includes a plurality of input units for letters or numerical figures for inputting said second identification information, and wherein the arraying positions of said letter input units are variable," as recited in Appellant's claims. In Lillibridge, the characters are variable. The arraying positions of the letter input units are not.

Still further, the Examiner again appears to be attempting to reconstruct Applicant's claimed invention in hindsight. There is no proper motivation the various references in the fashion offered by the Examiner.

Appellant respectfully requests reversal of the Examiner's rejection of claims 10-12, 22-24, and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Nemirofsky in view of Schneier II, and further in view of Lillibridge.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132, or additional evidence entered by or relied upon by the Examiner is being submitted.

X. RELATED PROCEEDINGS

No related proceedings are referenced in section II above, or copies of decisions in related proceedings are not provided, hence no Appendix is included.

Appellant believes no additional fee is due with this Brief. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2356 from which the undersigned is authorized to draw.

Dated: 1/17/07

Respectfully submitted,

By________________________ 57,199
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
Attorney for Appellant

APPENDIX A

1. (Previously Presented) An authentication system, said authentication system comprising:

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication_device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

2. (Previously Presented) The authentication system according to claim 1 wherein said authentication device includes:

decoding means for decoding the second identification information encrypted by said encrypting means based on said encryption key information,

said authentication device decoding the received encrypted second identification information based on said encryption key information, said authentication device comparing the decoded second identification information to the second identification information stored in said second identification information storage means, by way of performing the authentication.

3. (Previously Presented) The authentication system according to claim 2, wherein said second identification information is a password of a service user made up of a preset letter string or a preset string of numerical figures,

4. (Previously Presented) The authentication system according to claim 3 for authenticating the service user to whom preset services are offered from a service provider in a credit sale system,

an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

5. (Previously Presented) The authentication system according to claim 4, wherein said first and second communication means are wireless communication means.

6. (Previously Presented) The authentication system according to claim 4, wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently.

7. (Previously Presented) The authentication system according to claim 6, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.

8. (Previously Presented) The authentication system according to claim 6, wherein said second identification information stored in said transient storage means is erased every preset time interval.

9. (Previously Presented) The authentication system according to claim 6, wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.

10. (Previously Presented) The authentication system according to claim 4, wherein said operating means in said portable card terminal includes a plurality of input units for letters or numerical figures for inputting said second identification information, and wherein the arraying positions of said letter input units are variable.

11. (Previously Presented) The authentication system according to claim 10, wherein the arraying positions of said letter inputting units are varied prior to the inputting of said second identification information.

12. (Previously Presented) The authentication system according to claim 10, wherein said operating means in said portable card terminal includes a display unit for displaying letters and a selection unit for selecting the letters displayed on said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected by said selection unit from among plural letters sequentially displayed on said display unit.

13. (Previously Presented) An authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable card terminal, said method comprising

an operating step of inputting a second identification information associated with a first identification information that discriminates said portable card terminal and that is stored in a first identification information storage means of said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device, and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal,

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step, and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to the second identification information as stored in a second identification information storage means to perform the authentication.

14. (Previously Presented) The authentication method according to claim 13 further comprising

a decoding step of decoding the second identification information, encrypted in said encrypting step, based on said encryption key information,

the encrypted second identification information being decoded in said decoding step based on said encryption key information, and the decoded second identification information being compared to the second identification information stored in said second identification information storage means by way of performing the authentication.

15. (Previously Presented) The authentication method according to claim 14, wherein the encryption key information comprises a random number.

16. (Previously Presented) The authentication method according to claim 15 for authenticating a service user to whom preset services are offered from a service provider in a credit sale system, an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being an authentication device contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

17. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal and the authentication device are interconnected by wireless communication means.

18. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal includes a transient storage step of transiently storing the second identification information.

19. (Previously Presented) The authentication method according to claim18, wherein said transient storage step stores the second identification information input in said operating step until authentication of said portable card terminal by said authentication device.

20. (Previously presented) The authentication method according to claim 18, wherein said second identification information stored in said transient storage step is erased every preset time interval.

21. (Previously presented) The authentication method according to claim18, wherein said operating step includes a step of erasing the second identification information stored in said transient storage step.

22. (Previously Presented) The authentication method according to claim 16, wherein said operating step includes a letter inputting step of inputting said second identification information, and wherein the second identification information is input in said letter inputting step via a plurality of letter inputting units the arraying positions of which are variable.

23. (Previously Presented) The authentication method according to claim 22, wherein the arraying positions of said plural letters in said letter inputting step are varied prior to inputting of said second identification information.

24. (Previously Presented) The authentication method according to claim 22, wherein said operating step includes a display step of displaying letters and a selection step of selecting the letters displayed in said display step, and wherein the second identification information input by said operating step is made up by a string of letters selected in said selection step from among plural letters sequentially displayed in said display step.

25. (Canceled).

26. (Canceled).

27. (Canceled).

28. (Canceled).

29. (Canceled).

30. (Canceled).

31. (Canceled).

32. (Canceled).

33. (Canceled).

34. (Canceled).

35. (Previously Presented) A portable card terminal authenticated by an authentication device, comprising,

first identification information storage means for storing a first identification information for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

communication means for communication with said authentication device wherein said communication including transmitting the first identification information from the portable card terminal to the authentication device, and receiving encryption key information from the authentication device in response to transmitting the first identification information, and

encrypting means for encrypting the second identification information input by said operating means based on said encryption key information received from said authentication device, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal.

36. (Previously Presented) The portable card terminal according to claim 35, wherein said encryption key information comprises a random number.

37. (Previously Presented) The portable card terminal according to claim 35, wherein the portable card terminal is issued to a service user by a service provider to offer preset services for said service user in a credit sale system, an inter-account instant payment system and E-commerce carried out over a preset network and is in the form of a card.

38. (Previously Presented) The portable card terminal according to claim 37, wherein said communication means are wireless communication means.

39. (Previously Presented) The portable card terminal according to claim 37, wherein said portable card terminal includes transient storage means in which the second identification information is stored transiently.

40. (Previously Presented) The portable card terminal according to claim 39, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.

41. (Previously Presented) The portable card terminal according to claim 39, wherein said second identification information stored in said transient storage means is erased every preset time interval.

42. (Previously Presented) The portable card terminal according to claim 39, wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.

43. (Previously Presented) The portable card terminal according to claim 37, wherein said operating means includes a plurality of letter inputting means for inputting said second

identification information, and wherein the arraying positions of said letter inputting units are variable.

44. (Previously Presented) The portable card terminal according to claim 43, wherein the arraying positions of said plural letters in said letter inputting means are varied prior to the inputting of said second identification information.

45. (Previously Presented) The portable card terminal according to claim 43, wherein said operating means includes a display unit for displaying letters and a selection unit for selecting the letters displayed in said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected in said selection unit from among plural letters sequentially displayed on said display unit.

46. (Previously Presented) An authentication system made up by a portable card terminal and an authentication device provided independently of said portable card terminal for communication with said portable card terminal, said authentication system comprising:

said portable card terminal, including

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means including display means for irregularly displaying letters included in a group of letters and selection means for selecting the letters making up a second identification information from among the letters irregularly displayed on said display means, said operating means inputting the second identification information associated with said first identification information, encryption means for encrypting the second identification information input by said operating means based on an encryption key information, and

first communication means for communication with said authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, including

second identification information storage means having the first identification information and the second identification information stored therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing the second identification information encrypted by said encryption means to the second identification information stored in the second identification information storage means; wherein

said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device through said first communication means, and the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.